QKDelephone

Presented by the **Qeys to Success**

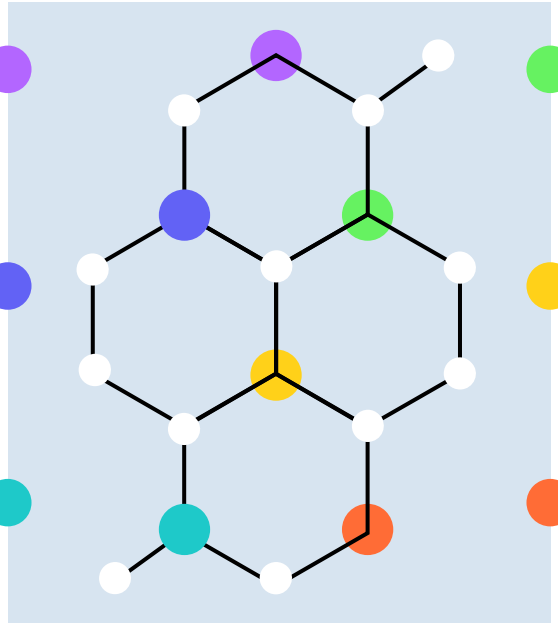
Aengus McGuinness, Krishnaveni Parvataneni,
Saarah Nazar & Swetha Kandeepan

Overview

01 **Introduction**
Quantum Key Distribution

02 **Our Game**
Fitting Quantum Key Distribution into Telephone

03 **Demo**
Running the Game on IonQ



04 **Impact**
Applications and Benefits of this Project

05 **Future Additions**
Methods to Scale Our Project in the Future

06 **Q&A**
Answering Audience Questions

Quantum Key Distribution

Sending

- Alice randomly selects **bits**
- Alice randomly selects **bases**
- Alice **encodes** bits into qubits
- Alice **sends** qubits to Bob

Receiving

- Bob randomly selects **bases**
- Bob **measures** qubits in those bases
- Bob **decodes** qubits to bits

Comparing

- Alice and Bob **compare** bases and bits
- They create their **key** (or make a new one if Eve is listening in)

Example of QKD

Sending

Let's say Alice randomly chooses these bits:
[1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0]

And these bases:
[Z, Z, Z, Z, Z, X, X, Z, Z, Z, X, Z]

Receiving

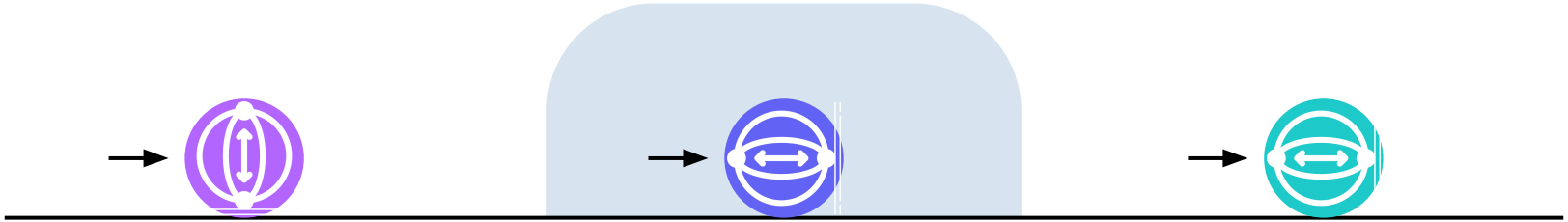
Then Bob measures the qubits
[1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0]

With these bases
[Z, X, X, X, Z, Z, Z, X, Z, Z, X, Z]

Comparing

Then they use the bits with the same bases:
[Z, X, X, X, Z, Z, Z, X, Z, Z, X, Z]
[Z, Z, Z, Z, Z, X, X, Z, Z, Z, X, Z]
Yielding these bits:
[1, 0, 1, 0, 1, 0]

How Our Game Works



Alice

Player #1

Alice sends a message to Bob, as she inputs a string, which is then encoded into bits

Eve

Player #2

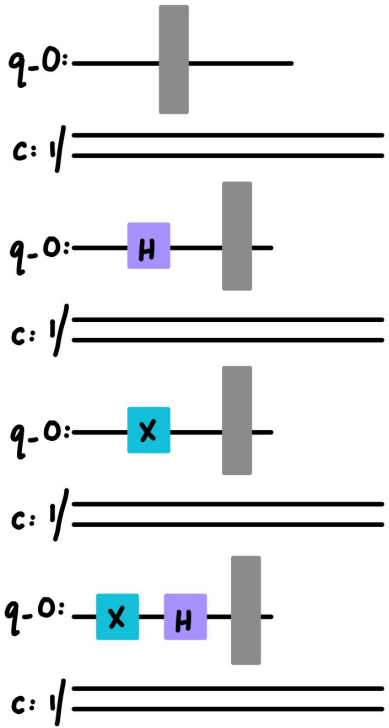
Sometimes, Eve tries to listen in on what Alice says, measuring the qubits and thus making them go into the wrong states

Bob

Player #3

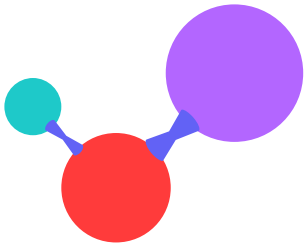
Bob gets Alice's message after Eve tries to eavesdrop, meaning that some of the bases are wrong for him, and he has to collaborate with Alice to figure out what is wrong

Game Demo



Impact

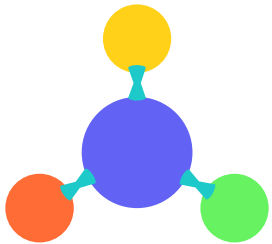
A



Educational

One of the main goals of our project was to make knowledge of QKD more widespread and allow for more people to access and be able to use a QKD algorithm

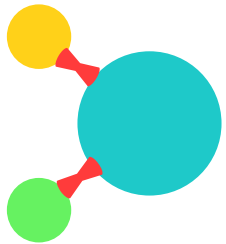
B



Information Security

This game is also a model for more secure information exchange, and such models, as an effect of the educational impact can have a great impact on Cryptography

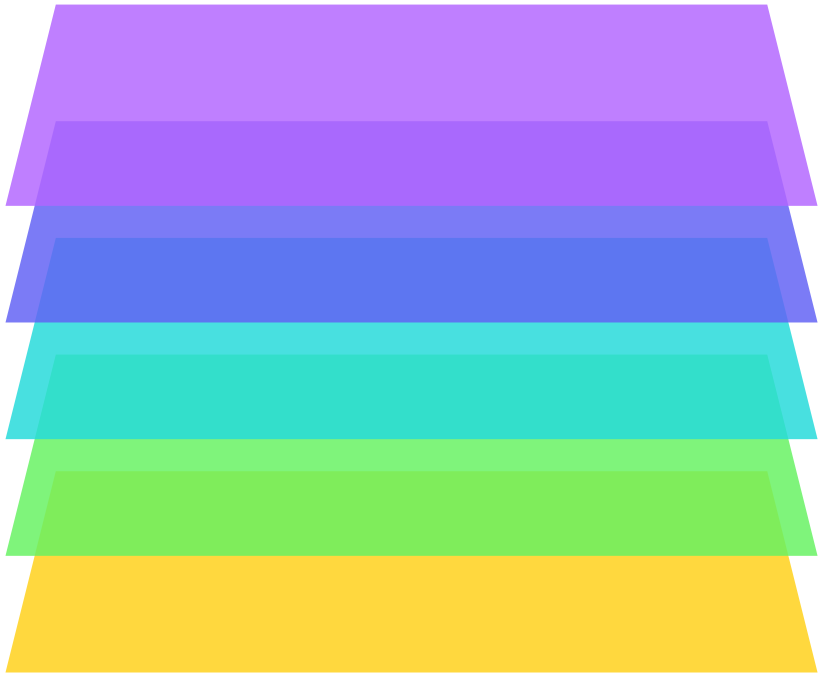
C



Entertainment

Our game is very similar to a game of telephone

Future Additions (and Implementations)



A

Make the game interactive

Using argparse to allow the user to choose number of interceptors and message

B

Graphical User Interface

Create a graphical interface through PyGame or cmu-graphics

C

More interactive players

Change the interceptors to actual people who can interactively eavesdrop

D

Optimize the number of bits

Find the most efficient number of bits and qubits for the QKD

E

Upload to a game platform

Upload a version of the game to an app store or another game hoster

Thank you for listening!

Any questions?